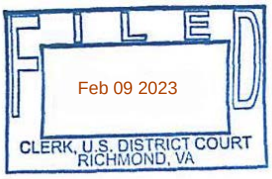
IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division



IN THE MATTER OF THE SEARCH OF VERIZON ACCOUNT 804-767-0266 THAT IS STORED AT PREMISES CONTROLLED BY SYNCHRONOSS TECHNOLOGIES, INC.

Case No. 3:23sw29

FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Kenneth Jordan III, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with Synchronoss Technologies Inc. Verizon account **804-767-0266** (hereinafter the "TARGET ACCOUNT") that is stored at premises owned, maintained, controlled, or operated by Synchronoss Technologies Inc. (hereafter "Synchronoss"), an Internet service provider headquartered at 200 Crossing Boulevard, 8th Floor, Bridgewater, NJ 08807, that provides cloud storage service for Verizon Wireless. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Synchronoss to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the TARGET ACCOUNT, including the contents of communications.

2. I am a sworn Special Deputy United States Marshal, Task Force Officer with the Federal Bureau of Investigation (FBI), United States Department of Justice, and have been since May 2018. I am assigned to the Richmond Field Office of the FBI in Richmond, Virginia, and

am responsible for conducting investigations pertaining to child exploitation. As part of my duties, I have received training regarding the investigation of federal crimes including crimes against children. By virtue of my assignment to the FBI Child Exploitation Task Force and with my employing agency (Middlesex County Sheriff's Office), I have performed a variety of investigative tasks including, but not limited to, conducting arrests and executing federal search warrants. As a Task Force Office and sworn Special Deputy United States Marshal, I am an investigative or law enforcement officer within the meaning of 18 U.S.C. § 2510(7). During my investigation, it was determined that Shawn Adams, hereafter referred to as the "TARGET," was the owner of the TARGET ACCOUNT. This was determined by the service of a subpoena to Verizon Wireless for subscriber records.

3. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that constitutes contraband, fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 2252A, specifically, Transportation, Distribution, Receipt, and Possession of Child Pornography (hereafter "the SUBJECT OFFENSES") are located on the TARGET ACCOUNT described in Attachment A. There is also probable cause to search the TARGET ACCOUNT described in Attachment A for evidence and instrumentalities of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, this Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

RELEVANT STATUTORY PROVISIONS

6. **Transportation of Child Pornography:** 18 U.S.C. § 2252A(a)(1) provides that it is a crime for any person to knowingly mail, transport or ship any child pornography using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer.

7. **Distribution or Receipt of Child Pornography:** 18 U.S.C. § 2252A(a)(2) provides that it is a crime to knowingly receive or distribute any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce, shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

8. **Possession of Child Pornography**: 18 U.S.C. § 2252A(a)(5) provides that it is a crime to knowingly possess, or knowingly access with intent to view, any child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

9. **Child pornography** means any visual depiction, in any format, of sexually explicit conduct where: (A) the production involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital or computer-generated image that is substantially indistinguishable from that of a minor engaged in sexually explicit conduct; or (C)

such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

10. **Visual depictions** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which are capable of conversion into a visual image, and data, which are capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. *See* 18 U.S.C. § 2256(5).

11. **Minor** means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

12. **Sexually explicit conduct** means actual or simulated: (i) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2).

BACKGROUND ON SYNCHRONOSS TECHNOLOGIES, INC.

13. Synchronoss Technologies, Inc. is the cloud-based storage provider for anything stored on the Verizon Cloud. Verizon Cloud offers secure online storage to back up and sync contacts, photos, videos, music, documents, call logs and text messages from Android mobile devices.

14. Synchronoss retains certain transactional information about the creation and use of each account on their systems. This information includes the date on which the images were uploaded into the cloud account, the methods used to connect to the account (such as device identifying information), and possible Wi-Fi captured IP addresses that could lead directly back to the address of the subscriber of the TARGET ACCOUNT. Because every device that connects to the Internet must use an IP address, IP address information can help to identify

which computers or other devices were used to access the TARGET ACCOUNT. This information can also serve to aid in identifying and locating the user of the account.

15. Internet service providers such as Synchronoss frequently provide reports regarding child abuse and child exploitation on their platforms to the National Center for Missing and Exploited Children ("NCMEC") or its international partner, the International Center for Missing and Exploited Children. *See* 18 U.S.C. § 2258A. These reports, known as CyberTips, provide useful information about when and how these providers become aware of violations of their terms of service and may provide information about other accounts associated with a subject's account. For CyberTips relating to the distribution, receipt or possession of child pornography, providers typically include copies of the offending images in their report submissions to NCMEC.

16. As explained herein, information stored in connection with the TARGET ACCOUNT may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with the TARGET ACCOUNT can indicate who has used or controlled the account. This user attribution evidence is analogous to the search for indicia of occupancy while executing a search warrant at a residence. For example, data files sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time.

17. Further, information maintained by the provider can show how and when the account was accessed or used. For example, as described herein, Synchronoss logs the IP addresses from which users access the account, along with the time and date of that access. By

determining, the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the cloud account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image and uploaded into the cloud account).

18. Lastly, stored electronic data may provide relevant insight into the account owner's state of mind as it relates to the offense under investigation. For example, information in the account may indicate the owner's motive and intent to commit a crime.

PROBABLE CAUSE

19. In October 2022 I was assigned numerous CyberTips including the 108 listed below. The original recipient of the first CyberTip (No. 111031912) was the Richmond Police Department (RPD). RPD investigated the CyberTip and determined that the TARGET was not in their jurisdiction and referred it back to Southern Virginia (SOVA) Internet Crimes Against Children (ICAC) Task Force Office, which was the entity that originally received the CyberTip from NCMEC and referred it to RPD. The SOVA ICAC subsequently determined that the TARGET resides in King William County King William does not have an investigator assigned to the SOVA Task Force, therefore the CyberTips were sent to me for investigation.

CyberTipline Report Numbers:

111031912	117540993	120440189	125881818
111684861	117599535	120498003	126114333
113688628	117701339	120887044	126350801
113906333	117755490	120954848	126705231
114332338	117794337	121009228	126761496
114406511	117838641	121190656	126945023
115136314	118031908	121262974	127041886
115261184	118151563	121561183	127092134
115494658	118239947	121814494	127155537

115878417	118309923	121999105	127255872
115940070	118364284	122086268	127345622
116117627	118412063	122174328	127398279
116277432	118661035	122251818	127477060
116451966	118722038	122405391	127574070
116514946	118786424	122578117	127646063
116588788	118865104	122708096	127712458
116686914	118932228	122843267	127773696
116840546	119132728	122930282	127830780
116947231	119173329	123112012	127893350
117025642	119306028	123235549	127939952
117159189	119375916	123707296	128030068
117238761	119563079	123927021	128143245
117289081	119732151	124385584	128247938
117346413	119953105	124479960	128291776
117392285	120153186	124574874	128409436
117438402	120275834	125276113	128477379
117488470	120386774	125663451	128717754

20. I personally reviewed the uploaded image files associated with the 108 CyberTips listed above. Based on my training and experience, I determined that the collection consists of a total of 1304 images of child pornography as that term is defined in 18 U.S.C. § 2256(8). Three examples of the images I reviewed are described below:

a. **File name: 1f0be326098545e29a1f9f129418fb3b_f578802eee154bcbaa0036a6f0dbdcf12f101ad4c4d38f09080598fbc09db015**: This image file, which is associated with CyberTip **No. 128717754** and was uploaded to the TARGET ACCOUNT on July 11, 2022, depicts a male of the approximate age of 12 years old. He is on a bed laying back on some pillows, has his hands behind his knees and is pulling them back and apart, exposing his anus and erect penis.

b. **File name: 1f0be326098545e29a1f9f129418fb3b_5717ded91dcb33cca3a2114cf2c532d4b40796905b2c16ead48700df85f0aaf9**: This image file, which is associated with CyberTip **No. 119953105** and was uploaded to the TARGET ACCOUNT on March 15, 2022, depicts a female of the approximate age of 14 months old lying with her legs outstretched and sucking on a pacifier while being penetrated vaginally by an inanimate object.

c. **File name**: **1f0be326098545e29a1f9f129418fb3b_cec7f6a10b001f2900227988f337695ccb3983e765d1da8abd1553000df0e8c4.zip:** This image file, which is associated with

> CyberTip **No. 116588788** and was uploaded to the TARGET ACCOUNT on January 12, 2022, depicts a female of the approximate age of six months old and lying on her back. An unidentified individual uses their index and middle fingers to spread the lips of the vagina wide apart exposing deep into the baby's vagina.

21. NCMEC received and generated the first CyberTip No. **111031912** on December 17, 2021, and the most current CyberTip, No. **128717754,** is dated July 11, 2022.

22. I have reviewed the returns of the subpoenas issued to Verizon Wireless and found that the phone number used to upload the child pornography images in all 108 CyberTip's was **804-767-0266**, i.e., the TARGET ACCOUNT. Pursuant to a subpoena served on March 25, 2022, Verizon provided subscriber information for the TARGET ACCOUNT. Verizon's records indicate that the TARGET ACCOUNT subscriber is Shawn Adams (i.e., the "TARGET"), with an address of 203 Forest Ct. Aylett, Virginia, email account of superman4life1982@gmail.com, and last four digits of his Social Security number of 5262.

23. Based on my review of records on file with the Virginia Department of Motor Vehicles, I confirmed that the address and last four digits of the Social Security Number that Verizon had on record for Shawn Adams are correct. Using another law enforcement tool available to me, TLOxp, I was able to confirm that Shawn Adams was also associated with the email address of superman4life1982@gmail.com.

24. Additionally, Verizon provided information that the device associated to the TARGET ACCOUNT was a Note 20 Ultra 5G Black 128GB, which is a Samsung Galaxy mobile device employing the Android operating system. Identification numbers for that device included an IMEI of 356556776814940 and IMSI of 311480657747842. The TARGET ACCOUNT was opened on October 6, 2021.

25. On February 2, 2023, this Court issued an earlier search warrant, Case No. 3:23-sw-16, for the TARGET ACCOUNT, which I promptly served on Synchronoss. On February 3,

2023, I received an email from a Synchronoss employee informing me that the TARGET ACCOUNT had been deactivated on July 12, 2022 (which I would note is the day after the most recent CyberTip), but that Synchronoss still possessed contents of the account because it had received a preservation request before the account had been closed. The Synchronoss employee also stated that Synchronoss's collection process is automated and cannot target specific dates. Because Synchronoss cannot filter searches by date they requested an amended warrant without a date range so that they could properly comply with the warrant.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

26. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Synchronoss to disclose to the government copies of the records and other information (including the data stored in the cloud account) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

27. Based on the forgoing, I request that the Court issue the proposed search warrant.

28. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

29. The government will execute this warrant by serving the warrant on Synchronoss. Because the warrant will be served on Synchronoss, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

30. Based on the forgoing, I submit there is probable cause for a warrant to search the TARGET ACCOUNT described in Attachment A for records and content constituting contraband, fruits, evidence, and instrumentalities of violations of the SUBJECT OFFENSES, as further described in Attachment B.

Respectfully submitted,

Kenneth H. Jordan III
TFO/Special Deputy U.S. Marshal
FBI Richmond Field Office

Sworn and attested to me by the Affiant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on February 9, 2023.

/s/ MRC
Mark R. Colombell
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies information associated with Verizon cloud account **804-767-0266** (the "TARGET ACCOUNT") that is stored at premises owned, maintained, controlled, or operated by Synchronoss Technologies, Inc., a company headquartered at 200 Crossing Boulevard, Floor 8, Bridgewater, NJ 08807.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Synchronoss Technologies, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Synchronoss Technologies, Inc., regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to Synchronoss Technologies, Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Synchronoss Technologies, Inc. is required to disclose the following information to the government for the TARGET ACCOUNT listed in Attachment A:

1. All business records and subscriber information, in any form kept, pertaining to the TARGET ACCOUNT, including:

    a. Names (including subscriber names, usernames, and screen names);

    b. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);

    c. Telephone numbers, including SMS recovery and alternate sign-in numbers;

    d. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, including login IP addresses;

    e. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, and alternate sign-in numbers;

    f. Length of service (including start date and creation IP) and types of service utilized;

    g. Means and source of payment (including any credit card or bank account number); and

h. Change history.

2. All device information associated with the TARGET ACCOUNT, including but not limited to manufacturer names, model numbers, serial numbers, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, international mobile subscriber identity (IMSI), FCC ID numbers, and telephone numbers;

3. Records of user activity for each connection made to or from the TARGET ACCOUNT, including, the date, time, length, and method of connection, data transfer volume, usernames, source and destination IP address, and all activity logs;

4. The contents of all media associated with the TARGET ACCOUNT, including stored or preserved copies of image and video files, in whatever format, sent to and from the TARGET ACCOUNT, any accounts with access to or which previously accessed each record, any location, device, or third-party application data associated with each record, and all associated logs of each record, including the creation and change history, access logs, and IP addresses;

5. Any and all email communications, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails, and all forwarding or fetching accounts relating to the TARGET ACCOUNT;

6. Any records pertaining to the user's contacts, including address books, contact lists, social network links, groups to which the user belongs or communicates with, user settings, and all associated logs and change history;

7. The contents of all text, audio, and video messages associated with the account, in any format and however initially transmitted, including stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history;

8. All location history indicating the location at which the account was active, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car), and associated logs and user settings;

9. Any abuse reports associated with the TARGET ACCOUNT;

10. Any report(s) regarding the account made to the National Center for Missing and Exploited Children ("NCMEC") including all data files and images submitted to NCMEC.

The Provider is hereby ordered to disclose the above information to the government within **14 DAYS** of issuance of this warrant.

I. Information to be seized by the government

All information described above in Section I that constitutes contraband, fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 2252A, specifically, Transportation, Distribution, Receipt and Possession of Child Pornography (hereafter "the SUBJECT OFFENSES") involving the user(s) of the TARGET ACCOUNT, including information pertaining to the following matters:

a. Evidence indicating violations of violations of the SUBJECT OFFENSES;

b. The identity of the person(s) who created or used the TARGET ACCOUNT, including records that help reveal the whereabouts of such person(s);

c. Evidence indicating the TARGET ACCOUNT owner's state of mind as it relates to the SUBJECT OFFENSES;

d. The identity and whereabouts of victims, coconspirators, accomplices, and aiders and abettors in the commission of the SUBJECT OFFENSES.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support

staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.